International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 7 Issue 3, May-June 2023 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Survey of Methods for Spotting Spammers on Twitter

Hareesha Devi, Pankaj Verma, Ankit Dhiman

Department of Computer Science, Arni University Kathgarh, Indora, Himachal Pradesh, India

ABSTRACT

Social networking sites' explosive expansion as a means of information sharing, management, communication, storage, and management has attracted hackers who abuse the Web to take advantage of security flaws for their own nefarious ends. Every day, forged internet accounts are compromised. Online social networks (OSNs) are rife with impersonators, phishers, scammers, and spammers who are difficult to spot. Users who send unsolicited communications to a large audience with the objective of advertising a product, entice victims to click on harmful links, or infect users' systems only for financial gain are known as spammers. Many studies have been conducted to identify spam profiles in OSNs. In this essay, we have discussed the methods currently in use to identify spam Twitter users. User-based, content-based, or a combination of both features could be used to identify spammers. The current paper gives a summary of the traits, methodologies, detection rates, and restrictions (if any) for identifying spam profiles, primarily on Twitter.

KEYWORDS: *Twitter, legitimate users, online social networks (OS's), and spammers*

How to cite this paper: Hareesha Devi | Pankaj Verma | Ankit Dhiman "A Survey of Methods for Spotting Spammers on Twitter" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-7 | Issue-3, June 2023, pp.694-702, URL: www.ijtsrd.com/papers/ijtsrd57439.pdf

IJTSRD57439

INTRODUCTION

A social networking site, according to Boyd et al. [5,] enables users to (a) create a profile, (b) befriend a list of other users, and (c) examine and navigate their own and other users' buddy lists. Through the use of Web 2.0 technology, these online social networks (OSNs) enable user interaction. These social networking sites are expanding quickly and altering how individuals communicate with one another. These websites have transformed in less than 8 years from a specialised area of online activity to a phenomenon that attracts millions of internet users. Online communities bring people with similar interests together, making it simpler for them to stay in touch with one another. Sixdegrees.com was the first social networking site to launch in 1997, and makeoutclub.com followed in 2000. Sixdegrees.com and while new websites like MySpace, LinkedIn, Bebo, Orkut, Twitter, etc. found success. Facebook, a very well-known website, was introduced in 2004 [5] and rapidly rose to fame throughout the globe. OSNs' greater user numbers make them more appealing targets for spammers and malevolent users. On social media websites, spam can take many forms and is difficult to identify. Anyone who has used the Internet has encountered spam of some kind, whether it is in emails, forums, newsgroups, etc. Spam [18] is defined as the practise of sending unsolicited bulk messages over electronic messaging systems. OSNs have grown in popularity and are now used as a platform for spam distribution. Spammers want to send product ads to users who are not connected to them. Some spammers post URLs that similar website had a short lifespan and quickely faded, lead to phishing websites where users' sensitive information is stolen. The detection of spam profiles in OSNs has been the subject of numerous papers. However, no review paper that consolidates the available research has yet been published in this sector. The purpose of our paper is to examine the academic research and work that have been done in this area by various scholars and to highlight the potential directions for future research. The methods for identifying spammers on Twitter have been researched and compared in this study, along with their presentation. The format of this essay is as follows: The approach used to conduct this review is described in Section 2, which is followed by a briefing on security issues in OSNs in Section 3. Spammers are defined in Section 4 along with their motivations; the introduction to Twitter and its risks is given in Section 5; the purpose of this survey study is covered in Section 6; the properties that can be used for detection purposes are covered in Section 7; A comparative examination of the research produced by various researchers is reviewed in Section 8; new researchers are given research recommendations in Section 9; and the review is concluded in Section 10.

METHODOLOGY

After conducting a systematic review using a principled approach and searching major research databases for computer science like IEEE Xplore, ACM Digital Library, Springer Link, Google Scholar, and Science Direct for relevant topics, the current methods for detecting spam profiles in OSNs were surveyed. We concentrated exclusively on studies published after 2009 since social networks were not conceptualised until 1997 [1], and only afterwards did they gain widespread acceptance. Then, in 2004 [1], Facebook was introduced, and it quickly gained popularity. As a result, it took some time for people to become accustomed to using these networks for communication, which is why these networks have been attacked. Over 60 papers were found after searching the five major databases mentioned above. After reviewing all of the paper titles and abstracts, the papers that will be reviewed for this survey were chosen. Only papers that were deemed appropriate for the current investigation were selected. 21 papers in total have been chosen for evaluation after publications with titles and abstracts relating to spam message detection and other unrelated areas were eliminated. The majority of the criteria used to identify spammers have been used to categorise the papers.

Through this essay, we're attempting to assemble a list of social networking papers we've read about identifying spam accounts on Twitter. The list is probably not comprehensive, but it lends shape to the ongoing study on identifying social network spammers. After reading this survey study, new researchers will find it simple to assess what research has been done, when, and how the current work may be expanded to improve spam detection. Every time it was appropriate, we included details on the methodology used, the dataset used, the features for spammer detection, and the efficacy of the strategies employed by different writers.

The papers discuss, in particular, the ramifications of spammers' interactions with members of social networks as well as current methods for identifying them.

SECURITY ISSUES IN OSNs

Online social networking sites (OSNs) are susceptible to security and privacy problems due to the volume of user data that these sites process daily. Social networking site users are vulnerable to a range of attacks:

1. Viruses - spammers utilise social networks as a distribution channel [19] for dangerous files to infect users' systems.
2. Phishing attacks: By pretending to be a reliable third party, users' sensitive information is obtained [30].
3. Users of social networks are bombarded with spam messages by spammers [11].
4. Sybil (fake) attack - attacker creates a number of false identities and poses as a real user in the system to undermine the reputation of trustworthy users in the network [20].
5. Social bots, a group of fictitious personas made to capture user information [32].
6. Attacks involving cloning and identity theft, in which perpetrators construct a profile of an already-existing user on the same network or across many networks in an effort to deceive the cloned user's friends [23]. Attackers will gain access to victims' information if they allow the friend requests provided by these cloned identities. Users and systems are overextended by these attacks.

TYPES OF SPAMMERS

The fraudulent users known as spammers put social networks' security and users' privacy at risk by tainting the data shared by legal users. One of the following categories best describes spammers [22]:

1. Phishers are people who act normally but are actually out to steal the personal information of other real users.
2. Fake Users: These are users who spoof real users' profiles in order to distribute spam to their friends or other network users.
3. Promoters: These are people that spread harmful links in advertisements or other promotional materials to other people in an effort to collect their personal data.

Spammers' motivations:

Promote pornography, spread malware, launch phishing attacks, and harm the reputation of the system.

TWITTER AS AN OSN

Introduction

Twitter is a social networking website with 500 million active users [14] as of today who share information. It was first introduced on March 21, 2006 [14]. Twitter's logo is a chirping bird, hence the name of the website. Users can access it to exchange frequent information called “tweets” which are messages of up to 140 characters long that anyone can send or read. These tweets are public by default and visible to all those who are following the tweeter. Users share these tweets which may contain news, opinions, photos, videos, links, and messages. Following is the standard terminology used in Twitter and relevant to our work:

Tweets [3]: A Twitter message that is no longer than 140 characters.

Followers and Followings [3]: Followers are users who a specific user is following, while Followings are people that a user is following.

Retweet [3]: A tweet that has been forwarded to a user's entire following.

Hashtags [3]: The # sign is used to annotate keywords or subjects in a tweet so that search engines may quickly find them.

Mention [3]: You can include replies and mentions of other users in tweets by using the @ sign in front of their usernames.

Lists [3]: Twitter offers a tool for grouping the persons you follow into lists.

Direct Message [3]: Also known as a DM, this refers to Twitter's mechanism for direct messaging users to communicate privately.

According to Twitter policy [16], signs of spam profiles include metrics like following a lot of users quickly,1 posting mostly links, using popular hashtags (#) when posting unrelated information, and repeatedly posting other users' tweets as your own. By tweeting to @spam, users have the option to report spammy profiles to Twitter. However, the Twitter policy [16] does not make it clear whether managers utilise user reports or automated processes to look for these circumstances, despite the fact that it is assumed that both approaches are used.

Threats on Twitter

1. Spammed Tweets [13]: Twitter only allows users to post tweets with a maximum of 140 characters, but despite this restriction, cybercriminals have discovered a way to make the most of it by creating succinct but compelling tweets that include links to promotions for free vouchers, job postings, or other promotions.
2. Downloads of malware [13]: Cybercriminals have shared tweets with links to websites where malware can be downloaded using Twitter. The Twitter worms that transmitted direct messages and even malware that attacked both Windows and Mac operating systems include FAKEAV and backdoor[13] programmes. KOOBFACE [13], a piece of social media virus that attacked both Facebook and Twitter, has the worst reputation.
3. Twitter bots [13]: Online criminals frequently utilise Twitter to run and manage botnets. These botnets threaten the security and privacy of the users by controlling their accounts.

Social Implications of OSNs

In addition to the typical issues that social networking sites bring for users, such as spamming, phishing assaults, malware infestations, social bots, viruses, etc., the biggest challenge is maintaining the security and confidentiality of private data.

Twitter policy states that if an account has more than 2,000 followers, this amount is constrained by the number of followers the account has.

Social networking websites are created with the intention of making information readily available and accessible to others. But tragically, cybercriminals exploit this information, which is readily accessible, to launch focused assaults. Attackers can easily find a means to gain access to a user's account in order to gather more information and use that information to gain access to the user's other accounts and the accounts of their friends.

MOTIVATING REVIEW

Social networks have been a target for spammers due to the simplicity of information sharing and the ability to stay up to date with current subjects. It can be challenging to identify such fraudulent individuals in OSNs because spammers are well-aware of the methods available to identify them. For the purpose of collecting money, spammers can utilise OSNs as the ideal platform to pose as legitimate users and attempt to convince innocent users to click on harmful posts. The most crucial area being researched by numerous experts is how to identify such people in order to safeguard the network and protect users' private information. In order to quickly evaluate the work that has been done in this field, researchers will find this paper to be of great assistance.

FEATURES DISTINGUISHING SPAMMERS & NON-SPAMMERS IN TWITTER

The papers analysed in this study are shown in Table 1, along with the type of features that were utilised to identify spam Twitter profiles. Spam and non-spam profiles can be distinguished by either user-based or content-based characteristics. In any social network, user-based features are the characteristics of the user's profile and behaviour, whereas content-based features are the characteristics of the text that users publish.

Table 1 Features for the detection of spam profiles

Attributes used for detection of spam profiles
User based features: which contain demographic information such as profile information, follower and following numbers, followers-to-followers ratio, reputation, account age, average time between tweets, posting habits, idle hours, tweet frequency, etc.[33,12,34,3,26]
Content based features: among them are the quantity of hashtags (#), the quantity of URLs in tweets, @ mentions, retweets, spam terms, HTTP links, trending topics, duplicate tweets, etc.[33,7,11,25]
User based and content based both [1,22,24,27,29,2,4]
Any additional features, such as graph connectedness or pictorial distance: Graph-based features, neighbor-based features, interaction-based features, social links, social activities, and Markov clustering method [21,9,28,33,23,6]

Function of the aforementioned features in identifying spam profiles in accordance with Twitter rules [16]:

1. The quantity of followers—spammers have fewer followers.
2. The amount of followers—Spammers frequently follow a lot of users.
3. Followers/Following Ratio: Spammers have a ratio of less than 1.
4. The ratio of followers to the total of followers and followings is referred to as reputation. Spammers are well-known.
5. Account age is calculated using the current date and the account's inception date. Since spammers typically create fresh accounts, this feature is less useful to them.
6. Average time between posts - In order to attract attention, spammers send out more tweets quickly.
7. Posting Time Behaviour: Spammers frequently post at predetermined times, such as early in the morning or late at night when real users aren't using social media.
8. Idle hours: Spammers continue to send messages to cut down on their idle time.
9. Tweet frequency: To attract other users' attention, spammers tweet more frequently and at unusual hours.
10. The quantity of hashtags (#) used by spammers to entice genuine users to read their tweets by posting numerous unrelated updates to the most popular topics on Twitter.
11. URLs: Spammers frequently tweet a big number of URLs to dangerous websites.
12. @mentions: In order to avoid being found, spammers use as many @usernames of unknown individuals as possible in their tweets.
13. Retweets are replies to any tweet that contain the @RT symbol, and spammers frequently utilise @RT in their tweets.less free time.
14. Spam Words – The majority of spammers' tweets contain spam words.
15. HTTP links - Tweets made by spammers contain the most www or http:// characters.
16. Duplicate tweets: Spammers frequently use many @usernames in their tweets to post identical tweets.

EXISTING METHODS FOR DETECTION OF SPAM PROFILES IN TWITTER

Researchers have employed a variety of strategies to identify the spam profiles in distinct OSNs. As Twitter is used to discuss and disseminate information about trending topics in real time rather than just as a social communication platform, we are concentrating primarily on the work that has been done to identify spammers on Twitter. The summary of the papers that were looked at about the identification of spammers on Twitter is shown in Table 2.

In 2010, Alex Hai Wang [1] made significant progress in the area of spam profile detection using both user- and content-based features. To find suspicious Twitter users, a prototype spam detection system has been presented. To investigate the "follower" and "friend" relationships, a directed social graph model has been put forth. Using a Bayesian classification technique, content-based characteristics and user-based features have been employed to make spam detection easier in accordance with Twitter's spam policy. The performance of numerous traditional classification techniques, including Decision Trees, Support Vector Machines (SVM), Naive Bayesian, and Neural Networks, has been compared using standard evaluation measures, and among all of them, the Bayesian classifier has been found to perform the best. The algorithm attained a 93.5% accuracy and an 89% precision across the 2,000 users in the crawling dataset and the 500 users in the test dataset. This method's limitation is that it was only evaluated on a very small dataset of 500 individuals by taking into account their 20 most recent tweets.

When Lee et al. [22] installed social honeypots made up of real profiles, they were able to identify suspicious users, and their bot gathered proof of spam by crawling the profile of the user who sent the unsolicited friend requests and URLs on Twitter and MySpace. Spammers have been identified using characteristics of profiles such as their posting habits, content, and friend information to build machine learning classifiers. Following investigation, profiles of users who contacted these social honeypots on Twitter and MySpace via unsolicited friend requests have been gathered. Spammers have been identified using the LIBSVM classifier. The approach's validation on two separate dataset combinations—10% spammers+90% non-spammers and 10% non-spammers+90% spammers—is one of its strong points. The approach has a drawback because fewer datasets have been utilised for validation.

Based on the content of tweets and user-based attributes, Benevenuto et al. [7] identified spammers. The following tweet content attributes are used: the quantity of hashtags per word, the quantity of URLs per word, the quantity of words per tweet, the quantity of characters per tweet, the quantity of hashtags per tweet, the quantity of numeric characters in the text, the quantity of users mentioned in each tweet, and the quantity of times the tweet has been retweeted. The features that set spammers apart from non-spammers include the percentage of tweets that contain URLs, the percentage of tweets that contain spam words, and the average amount of words that are hashtags on the tweets. 54 million Twitter users have been crawled, and 1065 users have been manually classified as spammers and non-spammers. Spammers and non-spammers have been separated using supervised machine learning, or SVM classifier. The system's detection accuracy is 87.6%, with only 3.6% of non-spammers incorrectly categorised.

Sending a message to "@spam" on Twitter enables users to report spam accounts to the company. Gee et al. [12] took use of this property and used a classification technique to find spam profiles. Both spam and regular user profiles have been gathered using the Twitter API and "@spam" in Twitter, respectively. The collected data was first represented in JSON before being provided in CSV format as a matrix. Users are rows in the matrix, and features are columns. Then CSV files were trained using Naive Bayes algorithm with 27% error rate then SVM algorithm has been used with error rate of 10%. Spam profiles detection accuracy is 89.3%. Limitation of this approach is that not very technical features have been used for detection and precision is also less i.e. 89.3% so it has been suggested that aggressive deployment of any system should be done only if precision is more than 99%.

McCord et al. [24] employed content-based features such the quantity of URLs, replies/mentions, retweets, and hashtags as well as user-based features like the quantity of friends and followers. Spam profiles on Twitter have been identified using classifiers including Random Forest, Support Vector Machine (SVM), Naive Bayesian, and K-Nearest Neighbour. The Random Forest classifier, which yields the best results after the SMO, Naive Bayesian, and K-NN classifiers, has been validated on 1000 users with 95.7% precision and 95.7% accuracy. As a result of the unbalanced dataset used and the fact that Random Forest is typically used in cases of unbalanced datasets, this approach's limitation is that reputation feature has been giving incorrect results for the considered dataset, failing to distinguish between spammers and non-spammers. Finally, the approach has only been validated on a small sample size.

Using two distinct features—URL rate and interaction rate—Lin et al. [28] identified persistent spam accounts in Twitter. Many different indicators, including the number of followers, number of followings, followers-to-following ratio, tweet content, number of hashtags, URL links, etc., have been utilised by the majority of publications to identify spam accounts. However, according to this study, all of these features are not very good at spotting spammers, hence only straightforward yet useful features like URL rate and interaction rate have been employed for identification. The ratio of tweets with URLs to all tweets is known as the URL rate, while the ratio of tweets that interact with one another is known as the interaction rate. Twitter API was used to crawl 26,758 accounts, and J48 classifier analysis was performed on 816 long-surviving accounts with an accuracy rate of 86%. The approach's limitation is that only two variables were utilised to detect spam profiles; hence, if spammers maintain low URL rates and low interaction rates, the system will not function as planned.

There are two different kinds of spammer detection systems, according to Amit A. et al. [2]: one is URL-centric, which relies on identifying fraudulent URLs, and the other is user-centric, which is based on features relating to people such followers/following ratio. The method used in this research is a hybrid one that takes into account both of the properties listed above. Along with an alert system to identify spam tweets, 15 new features have been proposed to catch spammers. Spammers' tweet campaigns and methods have also been researched. A dataset from Twitter with 500K users and another with 110,789 individuals were both used. Bait-oriented features, which highlight the strategies used by spammers to get victims to click on harmful links, include mentions to non-followers, trend hijacking, and trend intersection with well-known trends. Tweet interval variation, tweet volume variation, ratio of tweet interval variation to tweet volume variation, and tweeting sources are examples of behavioural characteristics. Duplicate URLs, duplicate domain names, and IP/domain ratio are examples of URL characteristics. Dissimilarity of tweet content, similarity of tweets, and URL and tweet similarity are all examples of content entropy properties. Follower/following ratio and the profile's description language dissimilarity are aspects of the profile. Then, using the Weka tool, all of these features were gathered from both malicious and benign users and fed into four supervised learning algorithms: Decision Tree, Random Forest, Bayes Network, and Decorate. With Decorate's classifier, which produces the best results, 93.6% of spammers have been found. It has been demonstrated that this method performs better than Twitter's spammer detection strategy. However, this method has only been tested on 31,808 individuals, whereas Twitter is taking into account millions of users.

A technique to identify abusive us ers that publish offensive content, including dangerous URLs, pornographic URLs, and phishing links, drive regular users from social networks, and violate their privacy has been presented by Chakraborty et al. [4]. The algorithm has two steps: the first checks a user's profile for offensive content before sending a friend request to another user, and the second checks the similarity of two profiles. If the user should accept a friend invitation after these two phases is up to the recommendation. This has been tested with a 5000 user Twitter dataset that was gathered using the REST API. Timing, content, and profile-based criteria are all taken into account when determining how to distinguish between abusive and non-abusive users. There have been SVM, Decision Tree, Random Forest, and Nave Bayesian classifiers employed. All classifiers are outperformed by SVM, and the model is operating at an accuracy of 89%.

New features were used by Yang et al. [6] to identify spammers on Twitter. There have been discussions of a number of evasion strategies used by spammers. Ten new detection features have been proposed, including three graph-based features, three neighbor-based features, three automation-based features, and one timing-based feature. These features are expensive and difficult to get around because they are based on techniques that spammers don't use to avoid detection and require more time, money, and resources. With the help of classifiers like Random Forest, Decision Tree, Decorate, and Bayesian Network, 18 features—eight already existent and ten new—have been examined for detection purposes. A Bayesian classifier's accuracy of 88.6% is the best. This method has a limitation in that very little data has been crawled and only a specific sort of spammers is being found with a low detection rate, which is the minimum number of spammers found in the dataset.

RESEARCH DIRECTIONS

During the survey, it became pretty clear that there has been a lot of work done to identify spam profiles in various OSNs. Even so, the detection rate can be improved by switching up the method and using more substantial features as the determining factor. The following are a few findings from the survey:

1. Considering that Twitter has millions of active users, and this number is growing. Additionally, almost all writers used a relatively limited testing dataset to evaluate the effectiveness of their methodology. Therefore, in order to evaluate the effectiveness of any strategy, the testing dataset must be expanded.
2. A multivariate model must be developed.
3. A technique that can identify all types of spammers must be developed.
4. It is necessary to test the methods using various mixtures of spammers and non-spammers.

Table 2 Outline of techniques used for thedetection of spammers

Author	Metrics Used	Methodology Used	Dataset Used	Results
Alex Hai Wang[1]	Graph Based and Content based	Compared Naive Bayesian, Neural Network, SVM and Decision Tree	Validatedon 500 Twitter users with 20 recent tweets	Naive Bayesian giving highestaccuracy - 93.5%
Lee et. al.[22]	User based	Compared Decorate, SimpleLogistic, FT, LogiBoost, RandomSubSpace, Bagging, J48, LibSVM	Validatedon 1000 Twitter users	Decorate giving highestaccuracy- 88.98%
Benevenuto et.al.[7]	User Based and Contentbased	SVM	Validated on 1065 Twitter users	Accuracy- 87.6% (with user based and content based features) and accuracy- 84.5% (with only user based features)
Gee et. al.[12]	User based	Compared Naive Bayesian, SVM	Validated on 450 Twitter users with 200 recent tweets	Accuracy- 89.6%
McCord et. al.[24]	User based and content based	Compared Random Forest, SVM, Naive Bayesian, K-NN	Validated on 1000 Twitterusers with 100 recent tweets	Radom Forest giving highestaccuracy- 95.7%
Lin et. al.[28]	URL rate, interaction rate	J48	Validated on 400 Twitterusers	Precision-86%
Amit A. et. al.[2]	Introduced 15 newfeatures	Compared Random Forest, Decision Tree, Decorate, Naive Bayesian	Validated on 31,808 Twitter users	Accuracy- 93.6%
Chakraborty et. al.[4]	User based, Contentbased	Compared Random Forest, SVM, Naive Bayesian, Decision Tree	Trained on 5000 Twitterusers with 200 recent tweets	SVM giving highest accuracy-89%
Yang et. al.[6]	18 features (8-existing & 10 newfeatures introduced)	Compared Random Forest, Decision Tree, Decorate, Naive Bayesian	Validated ontwo datasets- 5000 users and then 3500 users with 40 recent tweets	Bayesian giving highestaccuracy- 88.6%

CONCLUSION

Researchers have created and employed a variety of techniques to identify spammers on various social networks. The majority of the work has been done utilising classification approaches like SVM, Decision Tree, Naive Bayesian, and Random Forest, as can be inferred from the publications examined. User-based features, content-based features, or a combination of both have been used for detection. A few authors additionally added new detection features. All of the methods were only tried with a single combination of spammers and non-spammers and were validated on a very limited dataset. In comparison to employing solely user-based or content-based characteristics, combining features for the detection of spammers has demonstrated improved performance in terms of accuracy, precision, recall, etc.

REFERENCES

[1] Don't Follow Me: Spam Detection in Twitter, Proceedings of the 2010 International

Conference, Pages 1-10, 26-28 July 2010, IEEE.

[2] Amit A. Amleshwaram, Narasimha Reddy, Sandeep Yadav, Guofei Gu, Chao Yang, CATS: Characterizing Automation of Twitter Spammers, Texas A&M University, 2013, IEEE.

[3] Anshu Malhotra, Luam Totti, Wagner Meira Jr., Ponnurangam Kumaraguru, Virgılio Almeida, Studying User Footprints in Different Online Social Networks

[4] ,International Conference on Advances in Social Networks Analysis and Mining, 2012, IEEE/ACM.

[5] Ayon Chakraborty, Jyotirmoy Sundi, Som Satapathy, SPAM: A Framework for Social Profile Abuse Monitoring.

[6] Boyd, Ellison, N. B. (2007), Social network sites: Definition, history, and scholarship, Journal of Computer- Mediated Communication, 13(1), article 11, http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

[7] Chao Yang, Robert Chandler Harkreader, Guofei Gu , Die Free or Live Hard? Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers, RAID'11 Proceedings of the 14th international conference on Recent Advances in Intrusion Detection, Pages 318-337, 2011, Springer-Verlag Berlin, Heidelberg, ACM

[8] Fabricio Benevenuto, Gabriel Magno, Tiago Rodrigues, and Virgilio Almeida, Detecting Spammers on Twitter, CEAS 2010 Seventh annual Collaboration, Electronic messaging, Anti Abuse and Spam Conference, July 2010, Washington, US.

[9] Fact Sheet 35: Social Networking Privacy: How to be Safe, Secure and Social

[10] Faraz Ahmed, Muhammad Abulaish, SMIEEE, An MCL- Based Approach for Spam Profile Detection in Online Social Networks, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[11] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, Detecting Social Network Profile Cloning, 3rd International Workshop on Security and Social Networking, 2011, IEEE.

[12] Gianluca Stringhini, Christopher Kruegel, Giovanni Vigna, Detecting Spammers on Social Networks, University of California, Santa Barbara, Proceedings of the 26th Annual Computer Security Applications Conference, ACSAC ’10, Austin, Texas USA, pages 1-9, Dec. 6-10, 2010, ACM.

[13] Grace gee, Hakson Teh, Twitter Spammer Profile Detection, 2010.

[14] http://about-threats.trendmicro.com/us/webattack-Information regarding Twitter threats.

[15] http://en.wikipedia.org/wiki/Twitter-Information of Twitter.

[16] http://expandedramblings.com/index.php/march-2013-by-the-numbers-a-few-amazing-twitter-stats-Regarding statistics of Twitter.

[17] http://help.twitter.com/forums/26257/entries/1831- The Twitter Rules.

[18] http://twittnotes.com/2009/03/, 2000-following-limit-on- twitter.html-The 2000 Following Limit Policy on Twitter.

[19] http://www.spamhaus.org/consumer/definition-Spam Definition.

[20] J. Baltazar, J. Costoya, and R. Flores, “The real face of koobface: Thelargest web 2.0 botnet explained,” Trend Micro Threat Research , 2009.

[21] J. Douceur, “The sybil attack,” Peer-to-peer Systems, pp. 251–260, 2002.[12] D. Irani, M. Balduzzi, D. Balzarotti,

[22] E. Kirda, and C. Pu, “Reverse socialengineering attacks in online social networks,” Detection of Intrusionsand Malware, and Vulnerability Assessment , pp. 55–74, 2011.

[23] Jonghyuk Song, Sangho Lee and Jong Kim, Spam Filtering in Twitter using Sender-Receiver Relationship, RAID'11 Proceedings of the 14th International Conference on Recent Advances in Intrusion Detection, vol. 6961, Pages 301-317, 2011, Springer, Heidelberg ACM.

[24] Kyumin Lee, James Caverlee, Steve Webb, Uncovering Social Spammers: Social Honeypots + Machine Learning, Proceeding of the 33rd international ACM SIGIR conference on Research and development in information retrieval, 2010, Pages 435–442, ACM, New York (2010).

[25] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, Engin Kirda, All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks, International World Wide Web Conference Committee (IW3C2),

[26] WWW 2009, April 20–24, 2009, Madrid, Spain, ACM

[27] M. McCord, M. Chuah, Spam Detection on Twitter Using Traditional Classifiers, ATC'11, Banff, Canada, Sept 2-4, 2011, IEEE.

[28] Manuel Egele, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna, COMPA: Detecting Compromised Accounts on Social Networks.

[29] Marcel Flores, Aleksandar Kuzmanovic, Searching for Spam: Detecting Fraudulent Accounts via Web Search, LNCS 7799, pp. 208–217, 2013. Springer-Verlag Berlin Heidelberg 2013.

[30] Mauro Conti, Radha Poovendran, Marco Secchiero, FakeBook: Detecting Fake Profiles in On-line Social Networks, IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2012.

[31] Po-Ching Lin, Po-Min Huang, A Study of Effective Features for Detecting Long-surviving Twitter Spam Accounts, Advanced Communication Technology (ICACT), 15th International Conference on 27-30 Jan. 2013, IEEE.

[32] Sangho Lee and Jong Kimz, WARNINGBIRD: Detecting Suspicious URLs in Twitter Stream, 19th Network and Distributed System Security Symposium (NDSS), San Diego, California, USA, February 5-8, 2012.

[33] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," Communications of the ACM , vol. 50, no. 10, pp. 94–100, 2007.

[34] Vijay A. Balasubramaniyan, Arjun Maheswaran, Viswanathan Mahalingam, Mustaque Ahamad, H. Venkateswaran, A Crow or a Blackbird? Using True Social Network and Tweeting Behavior to Detect Malicious Entities in Twitter, 2002, ACM

[35] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbotnetwork: when bots socialize for fame and money," in Proceedings of the 27th Annual Computer Security Applications Conference. ACM,2011, pp. 93–102.

[36] Yin Zhuy, Xiao Wang, Erheng Zhong, Nanthan N. Liuy, He Li, Qiang Yang, Discovering Spammers in Social Networks, Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence.

[37] Zhi Yang, Christo Wilson, Xiao Wang, Tingting Gao, Ben

[38] Y. Zhao, and Yafei Dai, Uncovering Social Network Sybils in the Wild, Proceedings of the 11th ACM/USENIX Internet Measurement Conference (IMC'11), 2011.

[39] Verma, P., Khanday, A. M. U. D., Rabani, S. T., Mir, M. H., & Jamwal, S. (2019). Twitter sentiment analysis on Indian government project using R. Int J Recent Technol Eng, 8(3), 8338-41.

[40] Verma, P., & Jamwal, S. (2020). Mining public opinion on Indian Government policies using R. Int. J. Innov. Technol. Explor. Eng.(IJITEE), 9(3).

[41] Thakur, N., Choudhary, A., & Verma, P. Machine Learning Algorithms-A Systematic Review.

[42] Verma, P., & Mahajan, S. A Systematic review of Techniques to Spot Spammers on Twitter.

[43] Thakur, M., & Verma, P. A Review of Computer Network Topology and Analysis Examples.

[44] Kumar, A., Guleria, A., & Verma, P. Internet of Things (IoT) and Its Applications: A Survey Paper.